

Comment préparer les enfants aux Réseaux Sociaux ?



Comment
préparer
les
enfants
aux
Réseaux
Sociaux
?

Dangers de l'Internet au-delà de logiciels malveillants, ou l'enlèvement des données par des ransomware. Sur le Net, le respect de la vie privée est mis à mal par les réseaux sociaux, les moteurs de recherche et la publicité. Dans le cas des mineurs, il y a des risques plus inquiétants, dont ils ne sont pas pleinement conscients, mais leurs parents, les enseignants et la société doivent assurer leur sécurité. Une étude récente, appelé Kids Connected, et menée par la firme de sécurité Kaspersky Lab avec iconKids et jeunesse, révèle des faits troublants sur la façon dont les enfants se comportent en ligne. Comportements qui peuvent conduire à provoquer plus de crainte.

Ce rapport montre que **les enfants âgés de 8 à 16 ans sont accros aux réseaux sociaux**. En outre, l'activité peut les mettre en danger, eux et leurs familles. 35% des enfants disent qu'ils ne veulent pas être sans réseaux sociaux, et sont désireux de rejoindre des groupes en leur sein, ils sont en mesure de partager beaucoup d'informations personnelles. **Le problème** est qu'ils le font sans avoir conscience que les données qu'ils partagent sont vues par de nombreux utilisateurs et peuvent être utilisées par des personnes potentiellement dangereuses.

Trop d'informations personnelles

Mais **qu'est-ce que les mineurs partagent le plus** ? La plupart des enfants, 66%, **montrent l'école** où ils étudient, 54% **des lieux qu'ils visitent**, et 22% partagent même **la gestion de leurs maisons**. Mais, 33% des enfants donnent également des **informations sur les effets de leur famille et de leurs parents**, sur leur travail (36%) ou sur **ce que leurs parents facturent** (23% des enfants).

Mais, outre le partage des données réelles, **les mineurs sont également prêts à mentir sur le réseau**, et ils le font surtout **si ça peut leur ouvrir des portes**. Un tiers des enfants est prêt à mentir au sujet de l'âge. 17% des enfants font semblant d'être plus âgés, et de modifient leur âge en fonction du web ou le service qu'ils veulent utiliser, étant donné que beaucoup d'entre eux ont des restrictions (très facile à sauter) d'âge.

Avec ces données, **les cybercriminels disposent d'informations suffisantes pour être utilisés à des fins malveillantes**. Parmi les activités criminelles qu'ils pourraient commettre, ils trouvent l'emplacement physique des mineurs. **Tous les enfants doivent apprendre à un âge précoce ce qu'ils devraient partager en ligne**, ou non. Et connaître les paramètres des réseaux sociaux de la vie privée, de sorte que seuls leurs amis peuvent voir leurs publications et leurs données.

Comprendre quelles sont vos données et la façon de les protéger

Tous les enfants et leurs parents doivent comprendre ce que sont les données personnelles, et **la façon dont on peut les protéger**. "Ceci est comparable aujourd'hui à lire et à écrire", dit Janice Richardson, consultant senior chez European Schoolnet, qui explique que **«les enfants ont besoin d'apprendre à un âge précoce que la vie privée est votre bien le plus précieux, et un droit fondamental»**.

Comme des **conseils de base** qui sont donnés par Kaspersky Lab afin d'éviter autant que possible les risques:

- Une **bonne communication est essentielle**. Il faut parler aux enfants au sujet de leurs expériences et préoccupations.
- **Réalisez les premières étapes dans les réseaux sociaux avec eux** pour créer le profil, activez les options de confidentialité, publiez votre premier poste ...
- Les réseaux sociaux ont des **restrictions d'âge**. La plupart sont fixée à 13 ans. À cet âge, il est commode d'en profiter pour leur parler et leur expliquer leurs droits, les responsabilités et les préparer à l'entrée dans le monde numérique.
- Cela peut **devenir un jeu**, quelque chose que vous faites en famille: par exemple, l'impression de leur profil, accroché au mur, leurs postes ... Ils pourront visualiser le public à qui est destiné chaque contenu.
- **Établir des règles** pour leur utilisation.
- **Encourager les enfants à communiquer avec vous**, ils vous apprendront de nouvelles applications récemment installées, les services qu'ils utilisent ... Si cela devient une habitude depuis le début, il sera plus facile de partager des informations et de leur **parler de la vie privée et de sécurité**.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : La situation préoccupante des enfants dans le réseau: mentir pour accéder aux réseaux sociaux et y donner trop d'informations